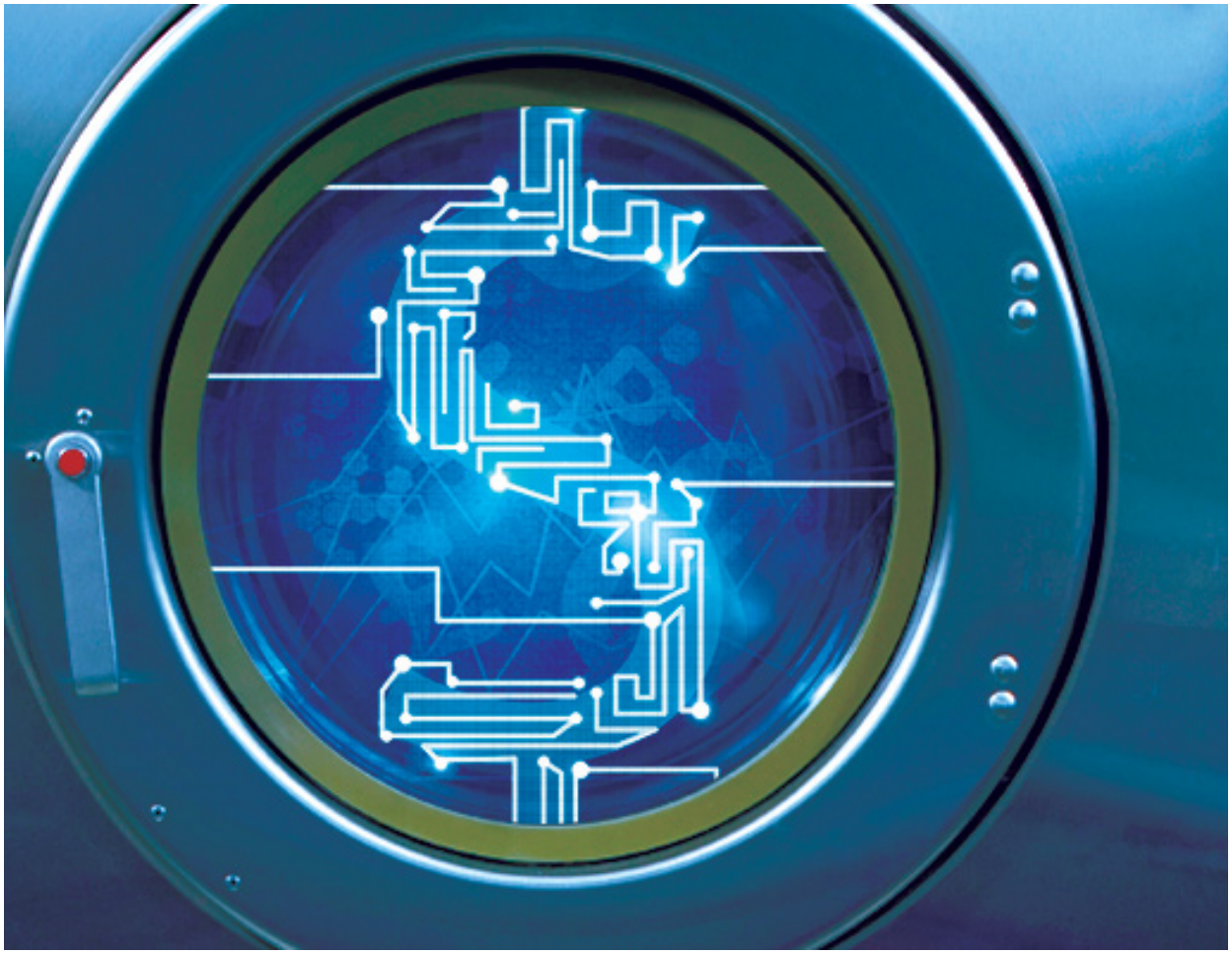
Online Exclusive

The virtual future of money laundering

June 2016

By Imran Khan, CAMS



On Jan. 20, Dutch police arrested 10 in the Netherlands as part of an international investigation into money laundering through sales of the virtual currency bitcoin, according to The Guardian article, Ten arrested in Netherlands over bitcoin money-laundering allegations (http://tinyurl.com/hmp2ll7). Criminals who work in the shadows of the dark web are often

currency, which is an attractive way to launder funds.

While today's leading virtual currencies, like bitcoin, may or may not pass the test of time, the underlying technology is here to stay. Innovators are taking us into a new realm in the exciting (and to some, terrifying) world of virtual currency. How do we prevent criminals from abusing the system in this still fairly new technology?

Money launderers historically have far outstripped the efforts of regulators, law-enforcement officials and anti-money laundering (AML) professionals who try to stop them from circumventing the law. Fraud examiners should seriously consider what the future of money laundering involving virtual currencies might look like so they can close the gap between the good guys and the bad guys.

Examining different types of virtual currencies and applications that have been developed around them gains us a better understanding of what makes them inherently high risk for money laundering and fraud.

eCache & TOR

Some virtual currencies, such as eCache, are completely anonymous. According to its operators, eCache doesn't link a person to their transactions; it works like a Digital Bearer Certificate (DBC) that can be transferred to another party just like any other data on the internet. (See Interview with eCache Operators (http://tinyurl.com/hr62k38), by Jonathan Logan, Dec. 17, 2007.) DBC is a combination of cryptographically encrypted data pieces (small part of the same data) that can later be decrypted and entitle the owner to a defined portion of assets backing the certificate.

Other virtual currencies, like bitcoin, store all transactions in a public ledger called "The Blockchain." The Blockchain only records the transactions, not the identities, of the users. It's possible to associate Internet Protocol (IP) addresses with bitcoin transactions; however, "The Onion Router" (TOR) can be used to hide a user's IP address, granting total anonymity. (See the paper, Onion Routing for Anonymous and Private Internet Connections (http://tinyurl.com/gl6pvn9), by David Goldschlag, Michael Reed and Paul Syverson, Jan. 28, 1999.) Onion routing hides online activity (http://tinyurl.com/zddwh2k) by sending securely encrypted messages through a distributed network of randomly selected proxy servers before they are delivered to their final destination. In an onion network, messages are encapsulated in layers of encryption — analogous to layers of an onion.

Dark Wallet

According to the *Wired* article, 'Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever (http://tinyurl.com/jzblxbj), by Andy Greenberg, April 29, 2014, this bitcoin application boosts virtual currency to another level by making it practically impossible to follow the trail of virtual currency via encrypting and mixing all user payments. "Dark Wallet," effectively makes bitcoin transactions totally untraceable.

Even Dark Wallet's developer, Amir Taaki, agreed in an interview that terrorist organizations could use his app — but he still backed his creation. According to the BBC News article, High Currency in the Dark Wallet (http://tinyurl.com/o35k6yv), by Jen Copestake, Sept. 19, 2014, Taaki said, "You can't stop using technology because of your personal bias. We stand for free and open systems where anybody can participate, no matter who you are."

The ability to conduct rapid and anonymous transactions through multiple jurisdictions makes virtual currency a very attractive tool to money launderers.

In the book Money Laundering: A Guide for Criminal Investigation (http://tinyurl.com/hn5gx6x), author John Madinger draws from the plot of the police action film "Lethal Weapon 2" to illustrate a loan-back money laundering scheme. In the movie, the criminal (character Leo Goetz) lends his own illegal funds to himself and washes them through the process of loan repayment. Goetz boasts that not only has he laundered the repaid money, but the interest payment is tax deductible as a business expense.

Imagine a similar loan-back scheme using a virtual currency — a reality that might not be too far away. Companies such as BTC Jam aim to connect lenders with borrowers globally using bitcoin as the currency. BTC Jam, which bills itself as the world's largest bitcoin peer-to-peer lending marketplace, also offers crowd-funding through this system, which opens the door to myriad possibilities for placement or layering of criminal funds.

Swarm

Crowdfunding can be used to launder money in several ways. For instance, an issuer might collude with investors (http://tinyurl.com/zsvgjq9) to exchange money for securities in a criminal enterprise in the name of a business transaction. As per a new FINCEN report (http://tinyurl.com/j3p388h), suspicious-activity reports have identified illicit use of crowdfunding platforms for money laundering, possible terrorist financing, credit-card fraud, identity theft, account takeovers, phishing schemes and shell company abuse.

Swarm, a crowdfunding startup, is similar to mainstream crowdfunding sites like Kickstarter or Indiegogo, but it uses bitcoin as its currency. It's an innovative concept, but fraudsters could potentially abuse it for money laundering and other criminal activities.

BitPay, Coinbase, Braintree and Circle

One of the greatest limitations of bitcoin has been that it can only be spent at a very small number of places. That's changing rapidly with companies such as BitPay, Coinbase and Braintree processing bitcoin for merchant payments. According to the CoinDesk article, BitPay Now Processing $1 Million in Bitcoin Payments Every Day (http://tinyurl.com/jqr4bxc), by Nermin Hajdarbegovic, May 28, 2014, BitPay's client base increased from 10,000 merchants to "more than 30,000 in just nine months."

The highly innovative Circle allows customers to obtain bitcoins with a credit card. (Coinbase, a competitor, provides a similar concept.) It's possible that very soon we'll have more startups that accept prepaid credit cards funded by cash.

Imagine this scenario: A criminal loads multiple prepaid credit cards with illicit cash and buys bitcoins. The criminal then uses these bitcoins to purchase goods and services online. All three stages of money laundering (placement, layering and integration) are displayed in this short example.

One of the serious challenges for investigators will be to follow the trail of criminal proceeds — especially when the whole process is done online — making it so much more convenient and opaque in comparison to traditional money-laundering methods. As virtual currencies become easier to process, we can anticipate that they'll be increasingly used in other high-risk industries such as casinos, online auctions, pawn brokers and used-car dealers.

A virtual capital market

Coloured Coins — which is beyond simple currencies — is an additional layer above the bitcoin network that uses existing bitcoins to represent other, potentially physical, assets. For example, transactions in the bitcoin Blockchain could be used to represent stock, securities or a deed to land. The startup businesses, ChromaWay and Colu, are among those attempting to bring Coloured Coins to a broader audience, according to Business Insider's article, The 25 most exciting bitcoin startups (http://tinyurl.com/htrnjez), by Rob Price, March 23, 2015.

Hedgy, which offers over-the-counter derivatives using Blockchain, is designed to assist the bitcoin community to hedge against price volatility. It's quite possible that one day we'll see financial derivatives from the commodities market traded in the Blockchain world.

As I previously discussed with DBCs, we could also see the return of bearer shares and bearer bonds (rarely seen in current capital market) in digital form. Bearer bonds are issued as paper and are payable to the bearer (holder) of the instrument. Consequently, their ownership isn't recorded with the issuer, which is convenient for criminals to move funds. With a DBC, the value is stored digitally and can later be used to transfer that value through email, instant messaging and SMS. Brokers could enter this virtual market, which would further complicate the basic Know Your Customer (KYC) process in the AML world of capital markets.

Virtual money service businesses

Criminals exploit money service businesses (MSB) at all stages of the money-laundering process. MSBs offer a full range of valuable financial services including currency exchange and money remittance services to people who might not have access to formal banking. But they pose a considerable threat as they often operate without proper registration or compliance regime, and transact with other overseas counterparts who are often unregulated. (See U.S. Money Laundering Threat Assessment (http://tinyurl.com/hfkaw32), December 2005, the report of a working group of the Departments of the Treasury, Justice and Homeland Security plus the Board of Governors of the Federal Reserve System and the U.S. Postal Service.)

Imagine a currency-exchange house operating in the virtual currency world: It's an exciting prospect for innovators in this industry but an idea that poses all kinds of questions about AML.

Anyone can use bitcoins to buy Litecoins (another virtual currency) via companies like BTC-E or Kraken. It won't be long before we have multiple virtual currencies being traded in virtual currency exchange houses. The fleeting nature of conventional client relationships with currency exchange houses coupled with the anonymity of multiple virtual currencies presents a dangerous money-laundering prospect.

BitGold, GoldMoney

BitGold (which was merged with GoldMoney Inc.) can help customers convert precious metal into virtual currency. According to the (intriguingly titled) *MoneyWeek* article, Don't touch this gold and bitcoin combo with a ten-foot bargepole (http://tinyurl.com/l4gcg36), by Dominic Frisby, May 19, 2015, BitGold models itself a sort of "PayPal for gold," which can be used in a coffee or grocery shop to buy everyday items or simply to buy and store gold.

Precious metals have been one of the most common methods of laundering funds because of demand, liquidity and transferability. Precious metals, especially gold, silver and platinum, have readily and actively traded markets and can be melted down, which obliterates refinery marks and leaves the source virtually untraceable. (See Assessment of Inherent

(Laundering and Terrorist Financing in Canada (http://tinyurl.com/hjmvbhe), Department of Finance Canada.)

It's reasonable to predict that speculators will use other virtual currencies to buy not only gold but all forms of precious metals and gems such as silver, diamond and platinum, which will make it even harder to trace criminal funds placed and layered through these companies.

MMORPGs

Many gamers use virtual currencies to participate in MMORPGs — Massively Multiplayer Online Role-Playing Games. Criminals use the virtual currency systems in these games in one country to send virtual money to associates in another country.

Jean-Loup Richet, a research associate at the ESSEC Business School, has gathered information on this topic from online forums in which criminals exchange tips. According to his findings, popular games for this type of scheme include Second Life and World of Warcraft. (See Laundering Money Online: a review of cybercriminals methods (http://tinyurl.com/jp7o2bb), by Richet, Oct. 9, 2013, Cornell University Library.) Undoubtedly, criminals' use of role-playing games for exchanging money with each other will only increase. They'll also exchange game-related virtual currencies with regular virtual currency systems such as bitcoin, Litecoin, Ripple, Paymer, Perfect Money etc. This will be very convenient for the layering stage of the money laundering process because it'll be easy to disguise the true origin of funds using rapid movement from one platform to another.

Combating the virtual threat

How can we prevent criminals or terrorists from abusing these new innovations? One common suggestion is to increase regulatory scrutiny. But we need more than overly simplistic answers such as this.

We have to thoroughly understand the virtual currency system because the solutions to stopping money laundering will likely emerge from innovations within the industry. For example, new Blockchain technology could be a powerful tool for record keeping, which can enhance KYC ability.

Companies can use Blockchain technology in poor or underdeveloped countries vulnerable to corruption. Factom, a Texas-based firm, has been working with the Honduran government (http://tinyurl.com/j6m5l55) to handle the registration and recording of land claims in a country with a history of susceptibility to land-title fraud. By using Blockchain, Honduras could potentially create a title system that's completely transparent as well as a permanent record.

It's crucial that we understand and embrace new technologies. By educating fraud examiners and others who fight money laundering in the virtual currency world, we can ultimately use these same technologies to turn the tables on money launderers and others who perpetrate fraud.

***Imran Khan, CAMS**, is a quality control & team lead – high risk team at BMO Financial Group. His email address is: imran.khan586@gmail.com (mailto:imran.khan586@gmail.com).*

The views and opinions expressed in this article are the author's own and do not necessarily represent his employer.

(/fm-home.aspx)

Related Articles

(article.aspx?id=4294991160)

The fluidity of credit card fraud (article.aspx?id=4294991160)

Chip technology, commonly called EMV (Europay, MasterCard and Visa), is being touted as one fix to this rising card-fraud epidemic. Chip cards use algorithms that are far more difficult than magnetic stripe cards to copy or breach, which can prevent criminals from stealing credit card data.

(article.aspx?id=4294989591)

Beware toll-road, Facebook and donation scams (article.aspx?id=4294989591)

One day Katie Calvin received an email informing her that she hadn't paid a recent toll fee and she had to pay immediately. She couldn't remember ever driving through a tollgate without paying. Good thing she didn't download the invoice and become the latest victim of this phishing scheme.

(article.aspx?id=4294989368)

The role of fraud examinations in cybercrime (article.aspx?id=4294989368)

Cyberbreaches and internal information theft are often regarded as information technology (IT) problems. However, most information loss isn't a pure-play IT issue, which might be part of data security problems. Should entities remove handling of cyberbreaches and information protection from IT?

Click here to Login and leave a comment...

Reviews

By Anonymous

(/fm-home.aspx)

(/article.aspx?id=4295001044)

March/April

View the Issue (/current.aspx)

Digital Edition (/article.aspx?id=4295001044)

Log in (/login.aspx?redirectURL=http://www.fraud-magazine.com/current-issue.aspx?pageid=611)

Member Services (mailto:MemberServices@ACFE.com) | Advertise (http://www.fraud-magazine.com/advertise-with-us.aspx) | Archive (http://www.fraud-magazine.com/archive-index.aspx)

(http://www.fraud-magazine.com/videos.aspx)

Fraud prevention starts at the top (http://www.fraud-magazine.com/videos.aspx)

Tony Prior, CFE, ACFE Regent, discusses the importance of a strong tone at the top for fraud prevention. View the video (http://www.fraud-magazine.com/videos.aspx).

ACFE Training & Events

Internal Controls for Data Security (Online Self-Study) (http://www.acfe.com/products.aspx?id=4294981165)

(/fm-home.aspx)
w.acfe.com/products.aspx?id=4294999366)

- CONTACT US (/CONTACT.ASPX)
- PRESS ROOM (//WWW.ACFE.COM/FOR-MEDIA.ASPX)
- ADVERTISE (/ADVERTISE-WITH-US.ASPX)
- ACFE BOOKSTORE (//WWW.ACFE.COM/PRODUCTLIST.ASPX)
- EVENTS & TRAINING (//WWW.ACFE.COM/TRAINING-EVENTS.ASPX)
- PRIVACY POLICY (/PRIVACY-POLICY.ASPX)

SUBSCRIBE (ABOUT-FRAUD-MAGAZINE.ASPX)

(mailto:FraudMagazine@acfe.com)

(https://www.facebook.com/AssociationofCertifiedFraudEx
fref=ts)

(https://www.linkedin.com/company/66541?
trk=tyah&trkInfo=clickedVertical%3Acompany%2CclickedE
1-4%2CtarId%3A1439826843694%2Ctas%3Aassociation%

(https://twitter.com/TheACFE?lang=en)

(https://www.instagram.com/theacfe/)

- ACFE Insights (//acfeinsights.squarespace.com)
- The Fraud Examiner (//www.acfe.com/the-fraud-examiner.aspx)
- Fraud Talk (//www.acfe.com/podcast/)

ACFE Global Headquarters: 716 West Avenue, Austin, TX, 78701-2727 USA